Accellion Share Securely™

Top 10 Reasons Federal Government Agencies Select Accellion Secure Mobile File Sharing Solutions

Accellion provides government agencies with secure mobile file sharing capabilities for enabling anytime, anywhere access to information while ensuring data security and compliance.

1. Proven Government Solution

Government agencies need solutions designed to meet their specific needs. Accellion has a proven track record of successfully providing US Federal agencies with secure mobile file sharing solutions that meet the strictest security requirements. The US Senate, NASA, USDA, Department of Veterans Affairs, and Securities and Exchange Commission are a few of the US Federal agencies currently using Accellion secure file sharing solutions.

2. FIPS Certified Encryption – Enhanced Data Protection

Government agencies require FIPS 140-2 certified encryption to ensure the protection of data in transit. The Accellion Mobile File Sharing Solution utilizes **FIPS-140-2 certified encryption**. Accellion has completed the rigorous validation process and obtained certification by the Cryptographic Module Validation Program (CMVP) to meet the security requirements set forth for Federal organizations by the National Institute of Standards and Technology (NIST).

All wireless "data in transit" is transmitted using FIPS 140-2 Certified Secure Socket Layer (SSL). With Accellion, government agencies are assured that all data downloaded to wireless devices is in full compliance with US Federal Government guidance and policy. Our certificate is available on the NIST website. All "data at rest" is also stored encrypted whether on a mobile device or on Accellion.

3. Private, Public, and Hybrid Cloud Options – Greater Flexibility

Today's nimble government agencies need solutions with flexible cloud deployment options, including the ability to deploy in a private, on-premise cloud. Accellion offers the widest breadth of cloud deployment options including private, public, or hybrid. Accellion is the #1 choice for private cloud/on-premise solutions enabling deployment in VMware, Microsoft HyperV and Citrix XenServer environments. With Accellion, agencies also have the ability to leverage NFS/EMC Atmos storage with their on-premise Accellion deployment.

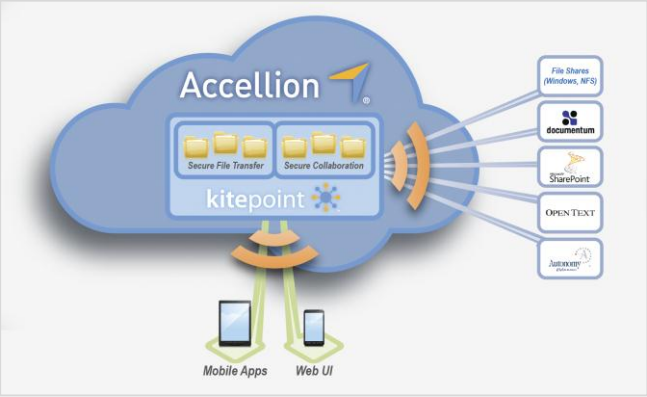
ACCELLION GOVERNMENT CUSTOMERS

For public cloud deployment, Accellion uses Amazon EC2, a solution that is rated FISMA Moderate ensuring US Federal agencies of policy compliance. Finally, Accellion provides a hybrid offering for those agencies requiring a combination of public and private cloud deployment.

4. Mobilize Enterprise Data – Secure SharePoint Access. No VPN

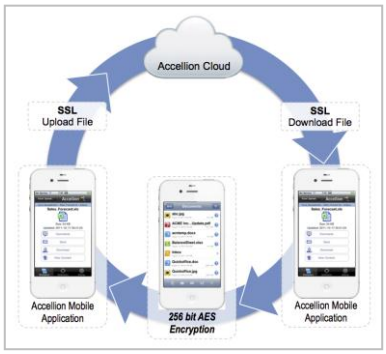
Government agencies require secure mobile access to content stored across enterprise content management (ECM) systems. Kitepoint provides organizations with secure mobile access to enterprise content stored in Microsoft® SharePoint and other enterprise content stores - anytime, anywhere, on any connected device without a VPN.

With kitepoint, users have a central hub for managing and accessing all their enterprise content – across silos of SharePoint sites, Windows File Servers, NFS, and other content stores. Kitepoint enables end-users to securely view and share content regardless of where files are stored, while IT can maintain control by enforcing security policies across all content stores for auditing, reporting, and compliance.



5. Native Accellion Mobile Apps – Secure Anytime, Anywhere Access to Data

For agencies requiring secure anytime, anywhere access to confidential information across devices, Accellion provides native mobile applications for Apple iOS (iPhone, iPad and iPod), Android, and BlackBerry OS. Accellion Mobile Apps provide agency employees secure viewing and sharing of enterprise content in secure workspaces. Users can create and share secure workspaces on mobile devices for on-the-go online collaboration. They can open and securely upload files from e-mails and other applications to Accellion secure workspaces.



With configurable user-access privileges, Accellion Mobile Apps allow IT to control which users can download, edit, and save files on devices for real-time collaboration and file sharing. Admins can whitelist applications used to open files from Accellion and also configure PIN access to the application. Files downloaded to the device by users are password protected and encrypted at rest with 256–bit AES encryption. Lastly, users can also directly upload image files to Accellion from the camera roll to easily and securely share via Accellion secure workspaces.

6. Centralized IT Control and Management – Greater IT Control

Government agencies require solutions that are not only easy for end-users, but also deliver the controls and management needed to ensure data security and compliance. Accellion offers a robust IT Admin Interface to enable IT to centrally manage and control thousands of users efficiently. Administrators can easily provision new users with appropriate user rights and privileges including setting up storage caps for workspaces, creating file and workspace retention policies, enabling/disabling mobile access and file sync capabilities for users, and enabling LDAP Groups to manage groups of users. Admins also have the ability to view comprehensive reports of all file and user activity. In addition to reporting, Accellion also supports email archiving and is compatible with industry standard mail archiving servers.

7. Enterprise Authentication – Greater Security

Strong authentication ensures that only authorized personel have access to data. Using Accellion, administrators centrally manage password policies as well as integrate with LDAP for authentication. Large agencies can integrate Active Directory / multi-LDAP to centrally manage and control user accounts across their entire deployment. Accellion also supports single-on through SAML (Secure Assertion Markup Language) 2.0 protocol, and Kerberos. Accellion supports multi-factor authentication through single sign-on providers.

8. Enterprise File Synchronization – Increased Security and Business Productivity

Today's 24/7 business climate demands that employees have secure access to the latest information across devices, online and offline. Accellion sync gives agency employees access to up-to-date files regardless of location or device, offline and online. Accellion file sync combines the ease of use of consumer solutions with the IT controls, security and management that government organizatons require. Unlike other solutions, Accellion offers flexible file syncing with kitedrive continous sync and workspace on-demand file synchronization so users can select how files are synchronized to optimize business productivity, network storage, and bandwidth. Files added to sync-enabled folders are synchronized with your cloud and then accessible across devices.

9. Outlook and Lync Integration – Increased Business Productivity

Government agencies require secure methods to share files from existing enterprise applications with both internal and external users. Using Accellion plug-ins for the Microsoft Productivity Suite, government employees can securely share files with internal and external recipients from within existing applications and without duplicating data.

Outlook Plug-in (included with Secure Mobile File Sharing)
Using the Accellion Microsoft Outlook Plug-in users can securely send files, up to 2GB in size per file, directly from within Microsoft Outlook. The file is delivered as a secure link. By clicking on the link and authenticating the recipient is able to download the file. If enabled by IT, the plugin also provides flexible end-user controls including the ability to set the file link expiration and control file access.

10. Secure Inter-Agency Online Collaboration – Increased Data Security

US Federal agencies require project and team collaboration for easy and secure information exchange within as well as across organizational boundaries for increased business productivity as well as reduced response time with real-time collaboration. With Accellion, users can create as many secure workspaces as needed, upload files, and then invite internal and external stakeholders to review, comment, update, share, synchronize, and send files securely to keep projects moving forward. To ensure data security, users can be assigned Manager, Contributor, Uploader and Viewer roles depending on the privileges required. Secure workspaces can be accessed from laptops, desktops, and mobile devices for anytime, anywhere collaboration. All data is encrypted with FIPS Certified SSL.

Accellion Share Securely™

Accellion, Inc.
1804 Embarcadero Road
Suite 200
Palo Alto, CA 94303

Tel +1 650 485-4300
Fax +1 650 485-4308
www.accellion.com
info@accellion.com